December 28, 2017

Michael Cohen, Director
California Department of Finance
915 L Street
Sacramento, CA 95814

Dear Mr. Michael Cohen,

In accordance with the State Leadership Accountability Act (SLAA), the Secretary of State submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2017.

Should you have any questions please contact Lizette Mata, Deputy Secretary of State, Operations, at (916) 695-1649, Lizette.Mata@sos.ca.gov.

BACKGROUND

The Secretary of State, a constitutionally established office, is the chief elections officer of the state and is responsible for the administration and enforcement of elections laws. The Secretary of State is also responsible for administering and enforcing laws pertaining to filing documents associated with California businesses, and is responsible for commissioning notaries public and enforcing the notary laws. The Secretary of State's office is home of the State Archives, preserving documents and records that have historical significance. The Secretary of State is the filing office for lobbying and campaign registration and disclosure documents filed under the Political Reform Act. The Secretary of State also operates the Safe at Home program, maintains the Domestic Partners and Advanced Health Care Directives registries, provides support functions for the Voting Modernization Board, and is home to the California Museum for History, Women and the Arts.

VISION AND VALUES

The vision of the California Secretary of State's Office is to be a recognized leader in ensuring fair and secure elections, making it easier to do business in California, and protecting individual rights and state treasures. We are committed to: service, ethics, teamwork, openness, innovation, and consistency.

MISSION

The mission of the California Secretary of State's Office is to:

- Support California business by registering and authenticating business entities and trademarks, enabling secured creditors to protect their financial interests, and regulating notaries public.
- Strengthen democracy by overseeing fair and accurate statewide elections, building confidence and participation, and providing public access to campaign and lobbying financial information.
- Protect individual rights by registering domestic partners and advance health care directives, and providing confidential mail forwarding services.
- Preserve California's history by acquiring, safeguarding, and sharing the state's historical treasures.

Policy associated with the administration of the Secretary of State is accomplished through the divisions of: Executive Office, State Archives, Business Programs, Elections, Information Technology, Management Services, and Political Reform.

Executive Office- The Executive Office is responsible for the Secretary of State's overall policy development and implementation and handles legislative, constituency, communications, project management and international relations issues. The office attests to the Governor's signature on executive orders, proclamations, resolutions, extradition papers and appointments. In addition, it chapters all bills passed by the Legislature.

Archives - The Secretary of State is responsible for safeguarding California's history in the State Archives. The Archive's staff collect, organize, and preserve the state's permanent government records and other historical materials such as maps, architectural drawings, photographs, video and audio tapes, and artifacts.

Business Programs- The Business Programs Division supports California businesses by registering and authenticating business entities and trademarks and enabling secured creditors to protect their financial interests. The division is responsible for filing documents associated with California corporations, limited liability companies, partnerships, limited partnerships and unincorporated associations, and pertaining to filing bonds and perfecting security agreements. The Business Programs Division processes millions of business filings and information requests each year.

Elections- The Elections Division oversees all federal and state elections within California. In every statewide election, California prepares voter information pamphlets in 10 languages for nearly 18 million registered voters. The Elections Division is focused on strengthening democracy by increasing voter turnout in California.

Information Technology- The Information Technology Division develops, delivers, and maintains information services and ensures date integrity by providing technical guidance to implement automated business solutions.

Management Services - The Management Services Division provides administrative and operational support necessary to effectively administer the Secretary of State's programs and includes the following functions: Fiscal and Budget Services, Purchasing, Contracts, Human Resources and Training, Information Security, and the Safe at Home program.

Political Reform - The Political Reform Division, under the statutory mandates of the Political Reform Act regulatory requirements and guidance issued by the Fair Political Practices Commission, helps make the political process more transparent by helping people monitor financing of state political campaigns and lobbying activities. Most candidates for state office, ballot measure committees, and anyone who lobbies the State Legislature and/or state agencies, must file detailed financial disclosure statements with the Secretary of State.

ONGOING MONITORING

As the head of Secretary of State, Alex Padilla, Secretary of State, is responsible for the overall establishment and maintenance of the internal control and monitoring systems.

Executive Monitoring Sponsor(s)

The executive monitoring sponsor responsibilities include facilitating and verifying that the

Secretary of State internal control monitoring practices are implemented and functioning as intended. The responsibilities as the executive monitoring sponsor(s) have been given to:
Lizette Mata, Deputy Secretary of State, Operations.

Monitoring Activities

Through our ongoing monitoring processes, the Secretary of State reviews, evaluates, and improves our systems of internal control and monitoring processes. As such, we have determined we comply with California Government Code sections 13400-13407.

The Secretary of State utilizes weekly Division Chiefs' meetings as a time for senior and Executive management to discuss items of significant impact to the agency, including current and potential internal control issues. In addition, Division Chiefs and Project Managers meet individually with the Deputy Secretary of State, Operations to discuss in greater detail, significant issues affecting each area of operations. The Deputy Secretary of State, Operations meets weekly with the Chief Deputy Secretary of State to elevate concerns and determine an appropriate plan of action. At this series of weekly meetings, continued monitoring and ongoing assessment of effectiveness of established controls are discussed.

Addressing Vulnerabilities

The Chief Deputy Secretary of State and the Deputy Secretary of State, Operations meet quarterly to discuss identified internal control deficiencies. This information is also provided to the Internal Auditor who, in turn, develops an audit plan for testing controls. The auditor addresses deficiencies found with the appropriate senior level manager, via an audit report, and requires a response, including the requirement that an implementation plan be developed within thirty days. The implementation plan includes measures to address the deficiency and the timeframe for implementation. The audit report, including the management response and implementation plan, are provided to the Chief Deputy Secretary of State. The Internal Auditor performs follow up testing and/or reviews to ensure corrective measures are in place based on time frames provided in the implementation plan and then reports back to the Chief Deputy Secretary of State.

Communication

Reports detailing the control activities associated with mitigating identified risks and their effectiveness are reported by each Division on a quarterly basis. These reports are then summarized and reported to the Chief Deputy Secretary of State and Counsel. The summarized reports are provided and discussed with the Deputy Secretary of State, Operations as well as Division Chiefs and their management teams.

Ongoing Monitoring Compliance

The Secretary of State has implemented and documented the ongoing monitoring processes as outlined in the monitoring requirements of California Government Code sections 13400-13407. These processes include reviews, evaluations, and improvements to the Secretary of State systems of controls and monitoring.

RISK ASSESSMENT PROCESS

The following personnel were involved in the Secretary of State risk assessment process: Executive Management, Middle Management, Front Line Management, and Staff.

Risk Identification

The Secretary of State's Risk Assessment was completed in accordance with Government Code sections 13400 through 13407. The Risk Assessment process included the highest levels of Agency leadership, and Program Managers (Division Chiefs), who are closely familiar with the functions, technology, processes, and risks in their respective areas.

The Secretary of State's office held a 2017 State Leadership Accountability Act report commencement meeting, attended by Agency Executive Leadership and Program Leaders, to address the work plan and timeline for completing the report. The work plan included five phases: 1) Risk Identification and Description 2) Leadership Evaluation 3) Controls Identification and Description 4) Leadership Review and 5) Report Submission.

1. During the Risk Identification and Description phase, each Program Leader completed a matrix to identify and describe risks based on impact to their program area, and the agency as a whole (high/medium/low), likelihood of occurrence (high/medium/low), what is affected (Operations, Reporting and/or Compliance), and the risk's origination (Internal or External). Meetings were held to address questions.
2. The Leadership Evaluation phase included discussion, examination, and determination of risks that could be identified for future monitoring.
3. During the Controls Identification phase, each Program Leader was asked to describe the control(s) already underway, and recommend new controls, to mitigate the risks in his or her areas.
4. The Leadership Review included discussion and consideration of controls that are partially in place and whether or not current technology and resources can be leveraged for better management of risk. Leadership determined if new controls are needed, or if enhancements are needed to existing controls.
5. Report Submission involved consolidating the Risks and Controls from each program area and preparing the report, within the guidelines provided by the Department of Finance.

The Risk Assessment process was carried out to ensure all levels of management were involved in the 2017 SLAA review. Risks were compiled, examined, and discussed to determine the risks that should be identified for future monitoring.

Along with any required implementation planning documentation, Agency leadership has given the responsibility of following up during the Ongoing Monitoring process to the Deputy Secretary of State, Operations and the Agency's Internal Auditor.

Risk Ranking

During the Risk Identification and Description phase, each Program Leader completed a matrix to identify and describe risks based on impact to their program area and the agency as a whole (high/medium/low) as well as the risk's likelihood of occurrence (high/medium/low). During the Controls Identification phase, each Program Leader was asked to describe the control(s) already underway, and recommend new controls, to mitigate the risks identified in his or her areas.

These factors were discussed and evaluated by Agency Leadership and taken into consideration during the Leadership Evaluation phase, when a complete list of agency risks were evaluated for their impact to the agency, their likelihood of occurrence, the control(s) already underway to mitigate the risk, and any recommended new controls.

Those risks with higher impact to the agency, a higher likelihood of occurrence, and/or insufficient or difficult to implement control(s) were ranked as the agency's highest-impact risks. Those risks with a medium impact to the agency, a medium likelihood of occurrence, and/or with new controls in need of implementation were ranked as the agency's mid-range impact risks. Those risks with the lowest impact to the agency, a lower likelihood of occurrence, and/or with sufficient control(s) already underway were ranked as the agency's lowest-impact risks. Those risks with the highest impact to the agency were identified for future monitoring.

RISKS AND CONTROLS

Risk: Operations -Internal-Technology—Support, Tools, Design, or Maintenance

The State Archives lacks a viable system for preservation of electronic records. The current system does not ensure preservation of historical resources existing solely in an electronic format. Historically important electronic records require a long-term records management and preservation strategy. The State Archives currently has a bare-bones system to accession process, and intake electronic records of long-term historical value and much in the electronic records that have been received remain inaccessible to the public. Storing records on CDs, DVDs, and external hard drives is not a viable long-term preservation strategy as these forms of media deteriorate rapidly. The State Archives houses more than 50 TB of data from state agencies, the Legislature, the executive branch, and the courts. The State Archives receives at least 15 TB per year and anticipates significant growth in this quantity as state agencies convert to digitized record copies and paperless environments.

The rate at which state agencies, the Legislature, and the Courts are creating born-digital records and digitizing existing paper records is increasing. Over the past few years, the State Archives has seen a greater quantity of electronic records with long-term historical value being added to the collection, at a rate of at least 15 TB per year. In previous fiscal years, resources have not been available to develop and implement an online transfer (ingest) portal for electronic records coming to the State Archives, leaving state agencies, the Legislature, and the Courts to transfer electronic records on CDs, DVDs, or external hard drives. This method of transfer leaves many electronic records on outdated media and increases the risk that data will deteriorate before it can be added to an OAIS system.

Limited resources have been available in previous years to allocate toward an OAIS system, though in 2016, the State Archives received funding to procure an annual subscription for an OAIS vendor system utilizing end of year funds. This system has a limited capacity of 50 TB per year and renewal and expansion is contingent upon available agency funds.

Without developing an online (ingest) portal, electronic records coming to the State Archives will continue to be transferred with CDs, DVDs, external hard drives, or other similar media, drastically increasing the risk that data could be lost or reside in an outdated format. Furthermore, without dedicated and sustained funding for the OAIS, the State Archives will not be able to fulfill its statutory mandate, public records will be lost, and public access to records will not be possible.

Until identified risks are addressed, the State Archives will not be able to read or access all the formats that constitute government records; read, append, or preserve all the records’ required metadata; ensure authenticity of electronic public records or meet legal requirements for their legal admissibility or accessibility; provide adequate security for statutorily restricted records; provide adequate access to public records in electronic form; preserve all historically valuable or vital electronic records; or respond to e-discovery requests in a timely manner.

Control A

The State Archives will adopt ISO 14721:2003, the international standard Open Archival Information System (OAIS) model, and identify and obtain or create an OAIS-compliant digital preservation, storage, and access system. The OAIS will become part of the State Archives' infrastructure for adequate control over electronic records and will include migration strategies for those records at greatest risk due to age and obsolescence.

Control B

In order to ensure that the infrastructure for electronic records preservation and access is adequate, the State Archives will seek more server storage space, or cloud storage, with redundancy built into the system.

Control C

The State Archives will develop a system in which electronic records can be digitally transferred from state agencies, the Legislature, and the courts to a secure ingest portal. This portal will allow electronic records to be appraised and those with long-term historic value saved to server storage space, or cloud storage, with redundancy built into the system.

Control D

The State Archives, in coordination with other state agencies, will conduct a survey to determine the quantity of statewide electronic records holdings at each agency. While all state records, regardless of format, should be managed throughout their entire life cycle, there are practical requirements surrounding the management and preservation of electronic records. Special attention and guidance is necessary to ensure their long-term viability and accessibility. The State Archives will work with state agencies to further update records retention schedules to be reflective of electronic records created by each agency.

Risk: Compliance-Internal-Resource Limitations

The State Archives has a limited ability to provide access to public records in an electronic format as outlined in CA Gov Code, Section 6253.9(a), due to inadequate staffing and electronic storage resources. The California Public Records Act (CA Gov Code, Section 6250-6270.5) requires that each state agency shall, "upon a request for a copy of records, shall, within 10 days from receipt of the request, determine whether the request, in whole or in part, seeks copies of disclosable public records in the possession of the agency and shall promptly notify the person making the request of the determination and the reasons therefor" (CA Gov Code, Section 6253(c)).

CA Gov Code, Section 6253.9(a) provides that, "Unless otherwise prohibited by law, any agency that has information that constitutes an identifiable public record not exempt from disclosure pursuant to this chapter that is in an electronic format shall make that information available in an electronic format when requested by any person." In the absence of an online transfer (ingest) portal for electronic records coming to the State Archives; state agencies, the Legislature, and the Courts have transferred electronic records on CDs, DVDs, external hard drives, and other media. Electronic records transfers on these media frequently come with little to no information about the content of the files and often contain file formats which are incompatible with current versions of program software.

As a result, there are many instances in which the State Archives must ask for the "unusual circumstances" extension outlined in CA Gov Code, Section 6253(c) to review electronic records on these CDs, DVDs, external hard drives, and other media. Significant staff resources are needed to upload electronic records from these media to a non-networked computer (clean machine), ensure the files are not corrupted and do not contain viruses, ensure that the file format is readable and accessible, and to check the records for content relevant to the California Public Records Act request. Without adequate staff resources and in the absence of a system in which the electronic records on these CDs, DVDs, external hard drives, and other media can be added and searchable, the State Archives has a limited ability to provide access to public records in electronic format.

Control A

In coordination with efforts directed at the 2017 SLAA Risk 1 - Insufficient system and Services, the State Archives will adopt ISO 14721:2003, the international standard Open Archival Information System (OAIS) model, and identify and obtain or create an OAIS-compliant digital preservation, storage, and access system. The OAIS will become part of the State Archives' infrastructure for adequate control over electronic records and will include migration strategies for those records at greatest risk due to age and obsolescence. The State Archives will further seek additional server storage space, or cloud storage, with redundancy built into the system to provide expanded access to electronic records through the Gencat public catalog.

Control B

The State Archives will research and implement processes to add or direct additional staff to California Public Records Act requests that require review of electronic records.

Risk: Operations -Internal-Physical Resources—Maintenance, Upgrades, Replacements, Security

The State Archives has insufficient facilities to ensure permanent preservation of historic resources and will soon run out of suitable space. The State Archives storage facility is currently at 83% of capacity. The Secretary of State is the custodian of the public archives of the State (Government Code section 12221). The State Archives has a State Records Appraisal Program to identify state agency records with permanent retention value. The records are maintained and made available for public inspection and research (California Public Records Act, Government Code sections 6250, et seq. and the California Information Practices Act, Civil Code sections 1798, et seq.).

The State Archives receives records from the executive, legislative, and judicial branches of California government and currently contains more than 125,000 cubic feet of records. On average, the State Archives projects a steady growth averaging 2.7% per year, with the annual rate of acquisitions (accessions) fluctuating with the lifecycle of records. Larger growth is due to higher numbers of records at the end of their retention period that are flagged to come to the State Archives. There is often an increase at the end of a legislative session or if the Appellate or Supreme Court transfer large quantities of case files in a given year. Accounting for average growth, plus one-time additions from state agency facility closures, end-of-term Governor's records, as well as pending large transfers from state agencies, the State Archives could add almost 30,000 cubic feet to its holdings by fiscal year 2019-2020, exceeding the capacity of the current facility. Once the State Archives building is full, state agencies will be responsible for preserving and maintaining records with long-term historic value that have been identified by State Archives staff.

Opened in 1995, the original plan for the State Archives building was to add two additional floors for records storage above the existing six-story structure. However, revised building codes and seismic upgrades prohibit upward expansion of the building. The State Archives collection currently contains more than 125,000 cubic feet of records and is at 83% of capacity. Based on growth projections and anticipated records transfers, it is estimated that the current State Archives building could run out of space by fiscal year 2019-2020. Storage shelves in the stacks consist of a combination of fixed and compact shelving. The State Archives has undergone several conversion projects to modify existing fixed shelving to mobile shelving, doubling the storage capacity. Based on the layout of the State Archives storage areas, two additional conversions of shelving are possible, providing several thousand additional cubic feet of storage. These spaces will need to be converted for the State Archives to avoid running out of space in the immediate future.

Once the State Archives building is full, state agencies will be responsible for preserving and maintaining records with long-term historic value that have been identified by State Archives staff. This will greatly increase the risk that essential records of state government could be damaged or lost and public access to these records may be limited if vendor-based off-site storage is utilized by an agency. The State Archives may have to decline taking records that document important programs and activities of state government and may not be able to receive or care for additional state agency vital records that are essential to the overall health of state government operations. The State might have to seek more expensive, less accessible commercial storage if the State Archives does not have adequate space.

Control A

The State Archives will continue to process collections to help reduce the volume of records permanently retained. A project is underway to reduce the State Archives' accumulation of unprocessed collections.

Control B

The State Archives will ensure that only records with historic value are received and permanently retained. The State Archives has begun eliminating records that have been identified as having no historic value. Nearly 1,000 cubic feet of records have been identified for deaccessioning. Second, an amendment to Government Code section 6268, effective January 2015, permits the State Archives to appraise Governors' records to identify those records having no historic value. The State Archives, through its California Records and Information Management (CalRIM) unit, is working with state agencies to ensure that only those records that have enduring value for preservation are being transferred to the State Archives.

Control C

The State Archives will continue to pursue the complete conversion of fixed shelving to mobile compact shelving as the most economical and efficient solution to meeting the State Archives' short-term space needs. The present building was designed and equipped for the conversion of fixed shelving to more space-efficient (mobile) shelving, which offers the highest possible density for storage of files and other media. The State Archives will develop a plan for converting an existing structure for off-site storage to meet the State Archives' long-term space needs.

Risk: Operations -Internal-Physical Resources—Maintenance, Upgrades, Replacements, Security

The State Archives' operational objectives would be disrupted and historical resources could be threatened or destroyed by a natural disaster. The emergency generator for the State Archives building is located below street level. Failure of the generator due to flooding could result in extreme temperature and humidity condition changes that would damage historical resources. These conditions could foster mold or mildew growth on the records, or could expose records to pests or other hazardous conditions.

Archival standards require that records be maintained at a constant temperature of 68 degrees +/- 2 degrees and constant humidity of 45% +/- 2%. If a power outage were to occur, under normal conditions, the emergency generator would provide backup power. Extreme temperature and humidity fluctuations caused by a generator failure would not only result in damage to unique and irreplaceable historical resources, but may prevent the evacuation of these resources to a temporary storage space or to receive salvage treatment. In the event of a complete energy failure, the freight elevators servicing the six stacks floors, where records are held, would be unusable. It would then be very difficult to evacuate heavy materials down the stairwells as neither carts nor pallets could be used and individual boxes would have to be hand carried by staff members -- a process which would be an extreme safety hazard and not recommended.

The State Archives collection storage areas (stacks) maintain constant conditions to stabilize and preserve the historic records. Continuous power is necessary to maintain the temperature of 68 degrees +/- 2 degrees and humidity of 45% +/- 2%. The emergency generator for the State Archives building is located below street level and leaves it vulnerable if a flood were to occur. Should the power be down and the emergency generator to become wet or unusable, the critical conditions for the stacks could not be maintained.

If the power to the building were to go down and the emergency generator was non-operational, extreme temperature and humidity condition changes may occur. This climate instability would result in damage historical resources. If the records were to become damp or wet, the unstable climate would result in mold or mildew growth on the records, or could expose records to pests or other hazardous conditions. Further, if the power and emergency generator were non-operational the records could not be evacuated to a temporary storage space or to receive salvage treatment because the freight elevators servicing the stacks would be unusable. Many of the records in the collection are heavy or oversized, leading to challenges evacuating the materials down stairwells. This process would be an extreme safety hazard and is not recommended.

Control A

The State Archives will consult with the Department of General Services on how to mitigate the risk of generator failure following a disaster that interrupts power to the State Archives building. The State Archives will consult with the Department of General Services and the Governor's Office of Emergency Services to plan for the appropriate response in the event of a disaster that causes power interruption and/or generator failure.

Control B

The State Archives will identify additional evacuation methods for high value records should the stack elevators be nonoperational before, during, or after an emergency.

Risk: Compliance-External-Responsibilities of Laws or Regulations Clarification

The State Archives has a limited ability to compel state agencies to identify records holdings, complete retention schedules, identify the useful life of records, and ensure records of enduring and historic value are transferred to the Archives. Without an enforcement mechanism, the Archives cannot ensure compliance with the State Records Management Act (CA Gov Code, Section 12270-12279) and State Administrative Manual, Section 1600, greatly increasing the risk that state and public records are not being properly cared for throughout the records lifecycle and that all records of historic value are not being identified or transferred to the Archives.

The State Records Management Act (CA Gov Code, Section 12270-12279) outlines the requirements for records management programs within state agencies. CA Gov Code, Section 12272 states that the duties of the Secretary of State shall include, but not be limited to, "Obtaining from agencies reports required for the administration of the program." This section allows the State Archives to request information from agencies but does not include an enforcement component that would compel state agencies to identify records holdings, complete retention schedules, identify the useful life of records, and ensure records of enduring and historic value are transferred to the Archives.

In the absence of enforcement language in the State Records Management Act (CA Gov Code, Section 12270-12279), the State Archives is unable to ensure that each state agency's public records are being properly cared for, retention periods appropriately applied, and records with long-term historic value are transferred to the State Archives. Without this language, it is probable that state agencies may be housing physical records in inadequate storage areas and may not be retaining paper or electronic records to the end of each retention period. Further, state agencies may not be reporting all types of public records created by program units on retention schedules, creating a significant risk that records with long-term historic value are not identified or transferred to the State Archives.

Control A

The State Archives will work with the SOS Executive Office to explore legislative options for adding an enforcement component to the State Records Management Act (CA Gov Code, Section 12270-12279) that would compel state agencies to identify records holdings, complete retention schedules, identify the useful life of records, and ensure records of enduring and historic value are transferred to the Archives.

Control B

Consistent with CA Gov Code, Section 12272, the State Archives will develop an annual survey in which state agencies will be asked to report on retention schedule status and use, vital records, quantity and content of records transfers of records to the State Records Center, quantity and content of records transfers to the State Archives, and agency records management coordinator training. The State Archives will compile the results of the survey and conduct site visits for agencies that require additional records management assistance or guidance.

Control C

In coordination with other state agencies, the State Archives will determine barriers and gaps in statewide records management practices. The State Archives will create and distribute updated tools, training, and resources to assist agency records management coordinators with effective records management execution.

Risk: Operations -Internal-Technology—Compatibility

The Business Programs Division (BPD) serves as the filing office for various statutorily authorized business related documents. BPD is operating in a paper environment and using multiple antiquated computer systems, creating processing delays & weakened internal controls in processing over two million paper documents and requests for information per year. The current systems and processes expose vital records to many risks. The foremost risk is the inability of the SOS to proficiently and promptly process these documents for California’s business community. BPD has an ongoing automation effort to modernize and automate these processes called California Business Connect (CBC), which will process these various business filings. In 2013, the Agency began receiving temporary funding to add limited term positions and to provide for temporary help and overtime to assist in reducing and maintaining and average turnaround time for business filings of five business days. With the additional funding and positions this goal has been achieved and turnaround times have vastly improved. Without this continued funding until CBC is implemented, turnaround times will increase again.

The BPD paper environment and the use of multiple antiquated computer systems and software tools create processing delays, resource constraints, and weaken internal controls in processing over two million documents and requests for information per year, including annualized volume growth and new filing types resulting from chaptered legislation.

The foremost risk is the inability of the SOS to proficiently and promptly process these two million documents and requests for information for California's business community. The SOS has received temporary funding to add limited term positions, to provide for temporary help and overtime to assist in reducing and maintaining an average turnaround time for business filings of five business days. Without continued funding until CBC is fully implemented, turnaround times will increase again.

Even with the additional temporary funding, the Secretary of State is not able to fully comply with the following legislative and regulatory mandates:

- Posting mandated public information to the Internet (California Corporations Code sections 1502 and 2117);
- Processing fees by SAM deadlines (SAM 8032.1); and
- Readily sharing vital information with government agencies for taxing, licensing, and regulatory purposes (various California Corporations Code and California Revenue and Taxation Code sections).

The predominantly manual paper processes and exclusive dependence on antiquated legacy information technology systems prevents the delivery of quick, effective, and efficient business services in the following aspects:

- Prevents effective and efficient delivery of services due to the lack of integrated information and databases;
- Makes the Secretary of State more vulnerable to having backlogs without the additional temporary funding and resources provided in the Budget Act of 2013 (Chapter 20, Statutes of 2013);
- Prevents other State agencies from having immediate access to the Secretary of State data and filings needed to assist them in their taxing, licensing, regulatory, and enforcement responsibilities;
- Increases the time it takes to locate and retrieve records;
- Increases length and types of staff training; and
- Requires numerous manual workarounds to perform statutory functions.

Control A

The SOS plans to implement the California Business Connect (CBC) information technology project. The CBC project will automate Business Entities, Uniform Commercial Code, and Trademarks, which encompasses approximately 100 different types of filing documents. The internal work processing efficiencies gained will be measured against baseline metrics already established for existing manual processing times and will be submitted to the Legislature after the first year of project completion. The CBC system will reduce unnecessary delays, provide a centralized and integrated single point of service for businesses, ensure a more secure processing of payments, provide online help in completing forms, and make services available 24 hours a day, seven days a week.

Control B

BPD will continue to initiate incremented improvements to mitigate submission volume, resource constraints, and processing goal risks: CBS - expanded/enhanced data and PDF images for free, LLC SI Online, Corp SI Online enhancement (June 2018), Trademarks Online (December 2017), and LLC

Formation Online (January 2018).

Risk: Compliance-External-Complexity or Dynamic Nature of Laws or Regulations

The Business Programs Division (BPD) files business formation documents for corporations, limited liability companies, and limited partnerships that are authorized to apply for state licenses associated with cannabis activities. As a result of the passage of the Medical Cannabis Regulation and Safety Act (MCRSA), the Control, Regulate and Tax Adult Use of Marijuana Act (AUMA), and the Medicinal and Adult-Use Cannabis Regulation and Safety Act (MAUCRSA), the SOS Business Programs Division (BPD) will experience an influx of new business entity and trademark filings related to cannabis activities requiring additional workload, customer contacts, outreach events, and coordination with other state agencies.

The SOS is the first stop in registering California businesses. Statutorily required business formation documents are filed with the SOS for corporations, limited liability companies, and limited partnerships that are authorized to apply for state licenses associated with cannabis activities and most applicants for licenses under Senate Bill (SB) 94's framework will first file business documents prior to seeking a license. Based on license projections from other California state agencies, SOS anticipates approximately 19,500 additional filings per year for cannabis-related business entities and an unknown volume of Trademarks. There already has been an unknown number of filings submitted where the cannabis related business is not identified either by its name or other provisions in the Articles. However, a significant amount of previously created cannabis business entities were formed under a nonprofit structure and trends indicate that many of these businesses will change to a for profit structure. Therefore, SOS anticipates both new formation filings and change filings to be among these 19,500 filings. In addition, SOS anticipates a high volume of Trademarks and Service Marks beginning January 1, 2018 when adult use cannabis becomes legal in California.

As requested by the Legislature, SOS's goal is to maintain business filing processing time of five (5) business days or less; however, current resource allocations are marginally sufficient to meet current demand (41% vacancy rate in the Limited Term classification or 20 out of 49 positions have been challenging recruitments due to the improving economy and unemployment rates). The cannabis volumes anticipated above will add additional stress to the current process flows due to increased filing volumes, customer contacts, outreach events, and required coordination with other state agencies resulting from the new industry and laws surrounding cannabis.

Control A

In addition to the June 2017 implementation of the SOS bizfile California website and Starting a New Business Brochure, an SOS cannabis website, including FAQs, cannabis business brochure, and checklist have been drafted to help educate customers on the steps needed to address their cannabis business concerns. Additionally, a new SOS form to facilitate the creation of new Cannabis Cooperative Associations and a form for Restated Articles of Incorporation - Mutual Benefit to General Stock (Form RST MU/GS) will be created. Finally, staff training and cross training on the new processes and forms is planned.

To help cannabis customers, the new SOS cannabis website, new forms, and training, are scheduled to be implemented in December 2017 and January 2018.

Control B

In order to meet the requirements of new cannabis related filings resulting from SB 94 and other new cannabis legislation, SOS will require the creation of new Attorney and Analyst positions and funding to manage workloads and document review associated with the new Cannabis Cooperate Association (including system modifications, testing, and implementation) and other cannabis-related filings, forms creation/modifications, phone calls, and outreach to customers and other agencies. A funding request for FY 2018/19 has been submitted.

Control C

BPD is also creating a new automated Trademark registration to mitigate cannabis submissions in early 2018.

Risk: Operations -External-Funding—Sources, Levels

The Business Program Division's (BPD) ongoing modernization and automation efforts and customer service levels could be impacted by a loss of spending authority from the Business Programs Modernization Fund (BPMF) and Business Fees Fund (BFF).

A loss of authority to spend BPMF and BFF on the development and maintenance of modernization and automation efforts (California Business Connect) and customer service levels will result in continued manual processing of paper-based filings and will negatively impact business in California and the legislatively recommended average 5 business-day turnaround. The BFF was established 1991 to support the programs from which the fees are collected. The BPMF was established via Assembly Bill 554 (Mullin) in September 2013 to support online Statements of Information.

If spending authority from the BPMF and BFF is lost or diminished, the programs from which the fees are collected and the development and maintenance of an online database will not be appropriately supported, business will be negatively impacted and the legislatively recommended average 5 business-day turnaround will be at risk. Further, funds not utilized for their intended purposes will be swept into the State's General Fund. Currently, any business fees in excess of the SOS expenditure authority is transfered to the General Fund except for $1 million that SOS is statutorily allowed to reserve.

Control A

Continued authority to spend from the BPMF and BFF in support of California Business Connect to modernize and automate current paper manual processes to provide appropriate customer service levels will mitigate this risk.

Risk: Operations -External-Staff—Recruitment, Retention, Staffing Levels

The Elections Division has experienced a consistent increase in demand for legal review of elections legal challenges, issues, and laws, which has burdened our two Elections attorneys as well as the Secretary of State's Chief Counsel. As a result, there is the potential of an increase in litigation, DOJ legal representation costs, and attorney fees (should we lose a case) due to our division lacking the resources to properly respond to legal issues and adequately comply with and/or implement applicable laws and regulations, and staff burnout. In addition, the legal issues have the potential to result in negative publicity as well as a lack of trust by voters in elections which could reduce citizen participation in our democracy.

There has been an unprecedented increase in attention to election administration over the years from the Florida Presidential Recount of 2000 cyber security concerns and most recently with the 2017 Presidential Advisory Commission on Election Integrity. As the nation's largest voting jurisdiction, California is subject to much of the attention as well as looked to as a nationwide leader in finding solutions. In addition, those who wish to change election policy nationwide often seek to use CA as a legal test case. As a result, the Elections Division has experienced a consistent increase in legal related matters, including civil lawsuits and appeals and Public Records Act requests, as well as media, citizen, and advocate inquiries. However, the Division lacks adequate legal services staffing levels to address the consistent increase in the demand and complexity of elections-related legal challenges, issues, and laws that must be reviewed/addressed.

The Chief Counsel is increasingly involved in election-related matters. As a result, he is overworked and not always available to assist with other agency related legal matters. Both the Chief Counsel and the Division's two attorneys are at risk of burnout and errors due to the overwhelming amount of issues to be addressed. The number of civil lawsuits and appeals have exponentially increased over the past two fiscal years, requiring the Department of Justice to increase its representation to the SOS. In turn, it has caused the SOS to exceed it's authority to pay the Department of Justice for legal services the last two fiscal years. Each case that goes to court, even with DOJ representation, requires additional work by the Division's attorneys and the Chief Counsel. Division staff have had to be redirected to assist Division legal counsel with the promulgation of statutorily required regulations, which has taken them away from their assigned duties. However, analytical staff will be unable to diverted during the election year. The SOS may be at risk of adequately ensuring the fair, accurate, and uniform administration of elections resulting in disenfranchisement of voters and an increase in legal challenges, including monetary damages, and negative publicity that could be damaging not only to the agency but to citizen participation in our democratic process.

Control A

The Executive office is hiring an additional attorney to be located in the Los Angeles office to assist the Chief Counsel, who may be able to assist in election-related matters.

Control B

Funding for an Attorney III, Attorney, and two Senior Legal Analysts was previously requested, but was denied. The Division will continue to work with the Executive Office to request additional funding for legal related positions to assist with the workload.

Risk: Operations -External-Staff—Recruitment, Retention, Staffing Levels

The Elections Division's staffing level is grossly inadequate in comparison to other states and has remained consistently low for at least the last 20 years, while there has been a consistent increase in the quantity and level of complexity of elections administration nationwide. Each year, the Division is consistently expected to do more with less. It has become consistently difficult to adequately train, retain, and recruit candidates into positions, particularly Elections Specialists, due to level of responsibility and workload expectations, including overtime. As a result, there is a higher risk of our Division not providing adequate oversight of and guidance to county elections officials, and a risk of staff burnout, absenteeism during critical election times, and errors, which all have high consequences.

There has been an unprecedented increase in attention to election administration over the years from the Florida Presidential Recount of 2000 cyber security concerns and most recently with the 2017 Presidential Advisory Commission on Election Integrity. As the nation's largest voting jurisdiction, California is subject to much of the attention as well as looked to as a nationwide leader in finding solutions. Each legislative session, without fail, brings a litany of new laws that affect the administration of elections, many of which are complex and some that affect very public processes mid-stream which must be immediately and seamlessly implemented. Each year, the Division staff level has remained relatively the same and is consistently expected to do more with less. In addition, election related programs and services are highly scrutinized by highly active and aggressive advocacy groups, candidates, legislators, the media, and the public. As a result, the Elections Division has experienced a consistent increase in legal related matters, including civil lawsuits and appeals and Public Records Act requests, as well as media, citizen, and advocate inquiries. However, the Division lacks adequate legal services staffing levels to address the consistent increase in the demand and complexity of elections-related legal challenges, issues, and laws that must be reviewed/addressed.

A lack of adequate election staffing can affect the SOS office's ability to ensure the fair, accurate, timely, and uniform administration of elections. Inadequate staffing levels affects our ability to ensure adequate oversight and guidance to county elections officials, for which our office was recently criticized in a BSA audit of Santa Clara County, implement ever-changing laws and processes, and meet the needs of all of our voters because we don't have the resources to adequately and timely address or study all of the issues that affect them. In addition, inadequate staffing results in staff burnout, absenteeism during critical election times, and errors. In other industries, there are acceptable error rates in publications and processes. However, there is no "acceptable" rate of error in elections. Information must be 100% accurate to ensure every voter is informed of their rights and understand state election laws and processes. Vote totals must be 100% accurate. One misidentified vote has the potential to affect the results of an election and who is seated for state or federal office. Incorrect information provided by staff or in printed material can ultimately result in costly lawsuits and the disenfranchisement of voters, and subject our office to negative political and public backlash.

Control A

The Division will continue to work with the Executive Office to request additional funding for positions to assist with the workload.

Control B

The Division conducts rigorous proofing and reviews of all election materials at multiple levels to mitigate the risk of errors. All public-facing materials are reviewed and proofed by staff, lead staff, attorneys, and management, at a minimum. Many are also reviewed by executive staff including the chief counsel and communications staff. When errors are made, they are immediately addressed and processes improved in order to prevent similar errors in the future.

Control C

The Division cross-trains its staff to ensure we mitigate risk of a single point of failure.

Risk: Operations -External-Litigation

The Elections Division does not currently have the resources to create and maintain a central tracking system for elections-related legal cases and issues.

The lack of a formal central tracking system creates additional workload for legal staff to research past issues and cases and their outcomes in order to determine how to address current and future issues of a similar nature.

In addition, there is the potential that beneficial information regarding past decisions and actions is lost or not accurately identified, which at a minimum may decrease efficiencies or, at worst, put the Agency at risk of unnecessary litigation and attorney fees. Furthermore, the lack of a tracking system limits the Division's ability to properly quantify workload and accurately request additional funding for positions.

Control A

The Division will continue to work with the Executive Office to request additional funding for the creation of a tracking system and a position to assist with populating and maintaining the database.

Control B

The Division could employ student assistants to create and maintain a tracking database. However, the work of student assistants would still require review by staff and could potentially create a union issue with student assistants doing the work of civil servants.

Risk: Operations -Internal-Technology - Data Security and Compatibility

The Information Technology Division (ITD) identified risks associated with outdated systems at the SOS that include: Operations (Technology - Data Security and Compatibility); Reporting (Distribution Limitation, Information Collected and Information Communicated); and Compliance (Complexity or Dynamic Nature of Laws or Regulations).

Outdated technology within the SOS is both a security issue and a hindrance to innovation. Legacy systems are increasingly difficult to maintain due to the age of the application language in which it is developed, and/or the system platform and hardware on which it runs. In most legacy systems, manufacturers have stopped producing security patches for operating systems and firmware hardware updates. Constant technological changes weaken the business value of legacy systems. Monolithic legacy architectures are antitheses to modern distributed, loosely-coupled and highly scalable architectures. In most cases, it is impossible to add new system functionality required by the Program and integrate with other systems and Internet-based business applications. In addition, ITD finds it increasingly difficult to recruit staff qualified to work on applications written in languages no longer found in modern technologies and nearly impossible to find training available for existing staff. Disparate legacy technical disciplines supported by ITD are performed by only one person, or the discipline is not staffed at all. Contracted staff or retired annuitants are relied upon to fulfill the role.

The potential consequences if a risk materializes include:

1. The threat landscape is continually changing and what seemed secure years ago may be demonstrably insecure today. Abandoned technology with insecure/out of date frameworks and libraries decreases security which could lead to data loss or data breach.
2. Most legacy systems are incompatible with newer systems. Timely access to data in legacy systems to integrate with modern application and technology can be very difficult and costly. This could impede SOS programs' ability to provide timely and accurate reporting.
3. Most legacy systems are prone to issues, which require periodic downtime for maintenance and bug fixes (if available). This downtime can impact the programs' ability to deliver services.
4. Increased user requests for new functionality on account of new regulatory requirements can induce "work around", which over time, can make legacy applications increasingly convoluted causing application instability.

Control A

1. A number of legacy systems and devices were decommissioned as November 2017 such as network devices, servers and workstations.
2. A legacy mission critical database was upgraded.
3. The Agency migrated to Microsoft O365 email services.

Control B

The Information Technology Division, Program Management Office and Program Divisions continue to work on the two reportable projects (CAL-ACCESS and California Business Connect (CBC)) to replace legacy systems.

- Political Reform Division (PRD):
    - The Enterprise Architect Team was hired in March 2017 to develop an enterprise architecture framework for the future state of the system that will be replacing CAL-ACCESS.
    - ITD, PMO, MSD and PRD are working together on the System Integrator Statement of Work (SOW) to replace CAL-ACCESS. The SOW was released in October 2017.

- Business Programs Division (BPD):
    - ITD, PMO and BPD are working on the CBC project to replace mainframe and legacy systems as well as manual processes. The project is currently on schedule to complete by 2021.
    - California Business Search - implemented in December 2016

Control C

The Secretary of State continues to assess resources to ensure highest priority projects and assignments are adequately staffed.

- August 2017 - ITD hired a web administrator to support the Secretary of State internal and external websites and BPD web applications.
- November 2017 - ITD hired a senior programmer to support the CARS project, which is to replace the legacy, CAL-ACCESS system.
- As of November 2017 - ITD is in the process of hiring, IT governance specialist, a server administrator with experience in Linux, an enterprise data architect with experience in databases, analytics and reporting, and an enterprise security architect.

Risk: Operations -External-Technology—Data Security

The Secretary of State Information Technology Division reports that risks to data security at the SOS include:

1. The unauthorized or accidental release of classified, personal or sensitive information;
2. All types of natural occurrences (e.g., hurricanes, earthquakes, tornadoes) that may damage or affect the system/application. Any of these potential threats could lead to a partial or total outage; thus affecting availability;
3. An intentional modification, insertion, deletion of operating system or application system programs, whether by an authorized user or not, which compromises the confidentiality, availability, or integrity of data, programs, systems or resources controlled by the system. This includes malicious code, such as logic bombs, Trojan horses, trapdoors, and viruses;
4. The accidental or intentional use of communications bandwidth for other than intended purposes;
5. An interference or fluctuation may occur as the result of a commercial power failure. This may cause denial of service to authorized users (failure) or a modification of data (fluctuation);
6. An intentional modification, insertion, or deletion of data, whether by authorized user or not, which compromises confidentiality, availability, or integrity of the data produced, processed, controlled, or stored by data processing systems;
7. An accidential configuration error during the initial installation or upgrade of hardware, software, communication equipment or operational environment;
8. Any communications link, unit or component failure sufficient to cause interruptions in the data transfer via telecommunications between computer terminals, remote or distributed processors, and host computing facility.

The risk could be caused internally within the organization or externally from intruders or other threats. The causes include:

1. Lack of comprehensive risk management strategy;
2. Lack of ongoing comprehensive security risk assessment;
3. Challenge in hiring qualified staff in the field of information security;
4. Malicious threats including computer viruses, Trojan, worm and spy-ware;
5. Spoofing at the data link and networking layer;
6. Denial of service attacks;
7. Hacker attacks;
8. Spam containing spy-wares;
9. Social engineering;
10. Physical attacks on the infrastructure;
11. Theft of data or equipment;
12. Vandalism;
13. Accidental threats like software or equipment malfunction or environmental mishap like flooding or fire;
14. Human error;
15. Software or hardware configuration error;
16. Software vulnerabilities; and
17. Lack of security policies and procedures.

The results of these risks may include:

1. Damage to the reputation of the organization;
2. Adverse media coverage;
3. Theft of sensitive data and adverse impact on the customers of the organization;
4. Disruption of services offered by ITD;
5. Damage to physical infrastructure;
6. Wastage of manpower in undoing damage;
7. Ongoing exposure if not remedied; and/or
8. Monetary or budget damages.

Control A

Establish a Risk Management Office led by the Agency Chief Information Risk Officer.

Because information technology assists and impacts every aspect of the business at the SOS, having a central risk management office, led by a qualified/certified information security hire will help alleviate the IT security risks. With new threats appearing every day, the work of identifying threats and countermeasures is continuous, and the effort in this regard is not effective if the responsibility is assigned to the existing staff who already have other assignments.

The Agency Chief Information Risk Officer will have the following responsibilities:

1. Information Systems Control Design and Implementation for the items listed below;
2. Information Systems Control Monitoring and Maintenance for the items listed below;
3. Monitor internal and external policy compliance;
4. Monitor regulation compliance;
5. Work with different departments in the organization to reduce risk;
6. Audit policies and controls continuously;

7. Detail out the security incident response program.

Control B

Risk Assessment - establish ongoing risk assessment of the following practices:

1. Organizational and Management - security program governance, confidentiality agreements, system security documentation, system certifications, configuration change control, security categorization, and vulnerability.
2. Personal - security awareness programs, HR security programs, and position categorization by access control.
3. Physical security - physical and environmental programs and controls and secure disposal of equipment.
4. Data security - disaster recovery planning, adequate information backup, monitoring, data classification, access controls, ensuring principle of least privilege, data storage and portable media protection.
5. Information security - identification and authentication and device identification and authentication policies and procedures, malicious code protections, intrusion detection, security alerts and advisories.
6. Software integrity - system and services acquisition safeguards and maintenance of software.
7. Personal computer security - device hardening, inactive computer device lock-out, and secure data storage.
8. Network protection - boundary, network infrastructure, and data transmission integrity.
9. Incident reporting and response.

Control C

Certification and accreditation controls -

1. Policies and procedures - covering security assessments, system certification, and system accreditation.
2. Security assessments - ensures information technology (IT) security at a standard and reasonable level relative to the business requirements.
3. Information system connections - controls and authorization to connect to other systems as required to support the organization.
4. Security certification - ensures security controls are effectively implemented through established verification techniques and procedures and provides confidence that appropriate safeguards and countermeasures are in place to protect the information system.
5. Plan of action and milestones - for the correction of any system shortcomings, which may be found by the security assessment, monitoring of activities, or security incidents.
6. Security Accreditation - the necessary security authorization of an information system to process, store, or transmit information that is required.
7. Continuous Monitoring - periodic monitoring of the system for problems by checking logs and performing preventative maintenance along with configuration management, and security assessments.

Control D

Security planning controls -

1. Policy and procedures - covers roles, responsibilities, scope, and compliance for all aspects of security for the organization including systems security, network security, and physical

security. The plan should be modified as conditions and technologies change.

2. System security plan - provides an overview of the controls and the risks associated with the system. The plan is reviewed and approved by designated officials.
3. System security plan update - system security plans are reviewed and updated either periodically or when modifications or new threats to the system warrant it.
4. Rules of behavior - communicated to all computer users usually through a computer systems appropriate use policy. The policy covers inappropriate use regarding non-business and use that may provide a security risk such as use of wireless equipment, creation of a different connection to the internet, use of file sharing programs, instant messaging, and other non-secure uses. Users sign a form stating that they have read the policy and agree to abide by it.
5. Privacy impact assessment - a privacy impact assessment is conducted on the computer system.

Control E

Awareness and training controls -

1. Policy and procedures - specifies who should be trained, subjects they should be trained about, and who is responsible.
2. Security awareness - ensures all users have basic knowledge about computer security awareness. The organization will determine the level of training required based on systems the user will access. This can be through enforcement of a computer training policy.
3. Security training - users are to receive training based on their roles in the organization. Users with a significant role dealing with system security should get more training in that area that users who do not deal with system security.
4. Security training records - records are kept of who has taken what training.

Control F

Configuration management controls -

1. Policy and procedures - assign responsibilities and provide procedures for changes to systems or software. Provide a mechanism to enforce compliance and a control to keep documentation current.
2. Baseline configuration - each system should have an established baseline configuration with documentation and an inventory of components including version numbers of all components.
3. Configuration change control - changes to systems is approved by appropriate officials.
4. Monitoring configuration changes - changes to systems are monitored and recorded. Analysis of the changes is done to be sure there are no adverse effects caused by the changes.
5. Access restrictions for change - prevents a conflict in change by only allowing one person to make changes at a time in the case of software.
6. Configuration settings - the configuration of systems is documented and monitored. The configuration settings are to be the most restrictive that still support the business case for security reasons.
7. Least functionality - this is basic server hardening where the running of unneeded services, port access, or programs is shut down on computer systems.

Control G

Contingency planning controls -

Define roles and responsibilities regarding contingency plan and procedures implementation, training and testing. A description of activities required to carry out the plan tied to the involved individuals roles is created and individuals are trained in their respective roles on a periodic basis such as yearly, or as the plan changes. The plan is tested using pre-defined exercises. A test results report must be generated and reviewed so corrective action may be taken. The plan should be reviewed annually and modified to suit business needs. An alternate site for data and equipment should be defined and secured using necessary agreements. An alternate site where hot or cold systems can be set up as part of the plan should be secured. Alternate telecommunications services should be identified and arranged to be made available. Information on all computer systems should be backed up to media and moved to an alternate location. Procedures for alternate system operation and system restoration must be created.

Control H
Accountability and audit controls -

Define roles, responsibilities, and compliance regarding auditing and addresses auditing of security controls including checking server maintenance and controls to make sure security policies are enforced. Auditable events include system events, application events, and security events including user logon and logoff times. Decisions must be made about which events should be monitored. Content of audit records should detail the time of the event, the event outcome, the event source, and the type of event. Systems must be managed to allow sufficient storage for audited events for a minimum period of time as specified by the organization. Management and administrators are notified when the system reaches its storage capacity limit. The system will need to be set to overwrite the oldest audit records, stop recording audits, or shut down. Audit logs are regularly reviewed and monitored for suspicious activity or events. Suspicious events or activities are investigated. Tools are used to expedite the use of the audit logs and the time of events are recorded. The logs are protected from unauthorized modification, deletion, or access.

Control I
System services and acquisition controls -

The methods of design of new systems, how major changes are made to existing systems, the design approval process, system support, resource allocation, documentation of systems, how outsourcing can be done, minimum requirements, and many more items should be defined in a system and services acquisition policy. Procedures should provide greater detail about who is responsible and step by step processes. Resources must be determined, documented, and allocated. The security requirements based on the business case must be determined. Items must be budgeted so resources are available to allow the system to meet business need. The system development lifecycle method must meet security needs. Security requirements are declared in acquisition contracts for acquisition systems. This includes guidance about products that are evaluated as secure along with information about required documentation, development practices, testing requirements, and other required security capabilities. Sufficient documentation should be provided about how to make the system more secure. Contractors must provide the same level of security and documentation in their products as is expected by the organization.

Control J
Software usage restrictions controls -

Only approved software can be used in the organization. Non-approved software such as peer to peer file sharing software or instant messaging software should not be installed on computers. A method to detect, block, or prevent installation of the software should be provided. Software is used in accordance with licensing. User installed software - Rules covering the downloading and installation of software is enforced. Allowed software is specified.

Risk: Operations -Internal-Technology—Compatibility

The Safe at Home program (SAH) currently uses outdated Sequel database software and Arrival software, which the SOS Information Technology Division (ITD) no longer supports. The Arrival software is used to scan the mail bins and print the mailing address on the envelopes. Recently, it was discovered that the Sequel reports used to generate the Annual and Monthly statistical reports were broken and the data reported was inaccurate. SAH staff worked with ITD to resolve and correct the problem; however, links continue to break. In addition, each time a new reporting requirement needs to be added to the database, the entire system is at risk of crashing. Pitney Bowes, the vendor for the Arrival software, has informed SAH that with each service call, it is getting increasingly difficult to connect the software to the printers. Should the database crash, SAH staff will no longer have the ability to enter participants into the database, generate reports, or connect to the Arrival software. This will leave SAH staff using peal-n-stick labels for mailing addresses and using spreadsheets to manually track the status of participants and corresponding change of addresses.

The SOS Information Technology Division (ITD) no longer supports the database software currently being used. Pitney Bowes has also advanced its software that is used in conjunction with the equipment used for mass mailing.

Should the SAH database or the Arrival software crash:

1. SAH will lose the ability to use the automated mail forwarding equipment resulting in participant mail delays;
2. Staff will need to prepare address labels and "peel-and-stick" each label on the forwarding envelopes;
3. Staff will not be able to enter information in the system and this information will need to be maintained by hand;
4. Staff will need to manually track participant renewal notifications; and
5. Documentation of phone calls will need to be kept in a hard copy file, making information sharing difficult among staff and inconvenient for the participant.

Control A

Purchasing more current software for both the database and the Arrival system; and then rebuilding the database (including the interconnection with the Arrival system) would resolve this risk.

Risk: Operations -External-FI$Cal Implementation, Maintenance, Functionality, or Support

The Management Services Division (MSD) is in the process of converting the SOS's accounting system from the State's current accounting system of record, CALSTARS, to FI$Cal.

FI$Cal does not retain any of the previous coding and reporting structure. In addition, it adds complexity to the coding structure and has added components to the records that were never tracked inside the system previously to increase transparency.

Based upon prior year release departments, the system in not fully functioning as expected and MSD will more than likely have to run dual systems for an unforeseen amount of time.

Control A

The workload related to conversion is a heavy lift and with no additional staffing allowed, this will more than likely result in the need for redirection of other departmental funding for procuring temporary assistance/overtime and or redirecting staff/vacancies.

Risk: Operations -Internal-Staff—Key Person Dependence, Workforce Planning

The Management Services Division (MSD) identified the lack of an Agency Succession Plan as a risk to SOS continuity of operations. In June 2016, MSD implemented the Succession Planning Task Force (SPTF) with members from the Executive Team and from each Division.

Following CalHR guidelines, the SPTF performed an analysis of the Agency's workforce using employment data from the State Controller's Office to identify the SOS workforce age and years of service. Currently, 47% of the Secretary of State's workforce is eligible for retirement, of which 28% are aged 55 years or older. An analysis of the Agency's organizational structure was also performed and key leadership and difficult to recruit positions were identified. Many retirement-age employees are in key leadership roles, or in positions that are difficult to recruit.

Retirement levels of this magnitude will likely adversely impact on-going operations as it will leave gaps in institutional knowledge as well as loss of specialized skills. Without a complete and comprehensive succession plan in place, the impact of employee retirements on operations will be significant due to the loss of experienced personnel.

Control A

Between January and June 2017, the SPTF analyzed the benefits, impact, and effort required to implement fourteen (14) strategies to address current and future leadership needs. Tools and templates were adopted to guide the Agency's succession planning practices. A comprehensive Succession Planning Program was developed and, in December 2017, the program was presented to and adopted by the Executive Team. In January 2018, employees will be surveyed to determine the baseline use of the five (5) selected strategies for implementation. The survey baseline data and implementation tools will then be provided to the Divisions for them to set goals, begin planning, and implement. Divisions will be required to improve the least-used strategy in each Division by 10% and to show an increase in the remaining strategies by June 2019. Additional surveys will be conducted to measure improvement. The long-term goal is to increase the use of the implemented strategies each year and add more strategies over time.

Risk: Compliance-External-Technology: Outdated, Incompatible

The SOS Office of Voting Systems Technology Assessment (OVSTA) identified aging voting systems throughout the state utilizing obsolete technology as a compliance risk and developed a funding plan to assist counties with system replacement.

The plan remains unfunded as of December 31, 2017.

If these voting systems are not replaced, the equipment in use will eventually break down to a state of non-repair, which will put the accuracy and reliability of California elections in jeopardy. Furthermore, as California is the most populous, complex, and diverse state in the nation, the repercussions of a voting system failure in California would be catastrophic, not only for state and local elections, but on a national level as well.

Control A

The Secretary of State developed a plan to fund new voting systems and technology throughout the state. The plan includes contracting with counties to allow them to develop a plan for replacing their current voting systems with new technology, employing methods that best meet the needs of their residents, as well as meet federal and state requirements. Funding will be allocated to each county based on a formula that will give equal weight to the number of persons eligible to vote, the number of registered voters, the average number of persons who voted in the last four statewide elections, and the number of polling places (all numbers will be based upon the June 7, 2016, Presidential Primary Election data).

The Secretary of State has been and continues to work collaboratively with the Department of Finance, the Legislature and the Governor's Office to pursue all options. In addition, the California Secretary of State sponsored Assembly Bill 668, the Voting Modernization Bond Act of 2018, seeking $450 million to improve California's voting systems.

Risk: Operations -Internal-Technology—Support, Tools, Design, or Maintenance

The Political Reform Division (PRD) currently uses a system called CAL-ACCESS, which provides for the viewing and reporting of accurate and consistent campaign and lobbying data by many customers and stakeholders. CAL-ACCESS employs an amalgamation of software, firmware and hardware all of which is past end-of-life, resulting in difficulties in supporting and maintaining the system. The system is unable to (or does not) enforce the reporting of accurate and consistent data; impedes the ability to respond to a dynamic legislative and regulatory environment; and poses a risk of failure with no assured path to timely recovery. Over the 15-year span of CAL-ACCESS operation, the system has become obsolete. From 11/29/2011 through the month of December 2011, CAL-ACCESS experienced an outage, during which time the public, including filers, were unable to access the system. CAL-ACCESS is no longer supported by vendors, posing a serious risk to recovery, if the system fails again.

As a result of the system's age and its original design features, it suffers these critical vulnerabilities: (a) Obsolete Platform and operating system, (b) Outdated and inflexible architectural design, and (c) Lack of software and system documentation.

If the CAL-ACCESS system fails again, it will impede the ability to respond to a dynamic legislative and regulatory environment, and poses a risk of failure with no assured path to timely recovery.

Control A

The SOS is in the process of replacing CAL-ACCESS, by means of the CAL-ACCESS Replacement System (CARS) project. Some of the key controls have been, (a) Subject Matter Experts (SMEs) have been selected to work on this project, (b) the Oracle9i database has been moved to 11g and CAL-ACCESS is now on a Windows platform, instead of an emulated True64 platform (c) Use Cases have been developed, (d) Business Rules are in the process of being created by contractors and SMEs, and (e) a Request for Offer #17-025 for a CARS Project System Integrator has been posted with an application deadline on January 8, 2018.

CONCLUSION

The Secretary of State strives to reduce the risks inherent in our work and accepts the responsibility to continuously improve by addressing newly recognized risks and revising controls to prevent those risks from happening. I certify our internal control and monitoring systems are adequate to identify and address current and potential risks facing the organization.

Alex Padilla, Secretary of State

CC: California Legislature [Senate (2), Assembly (1)]
California State Auditor
California State Library
California State Controller
Director of California Department of Finance
Secretary of California Government Operations Agency